PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-245657
(43)Date of publication of application : 19.09.1995

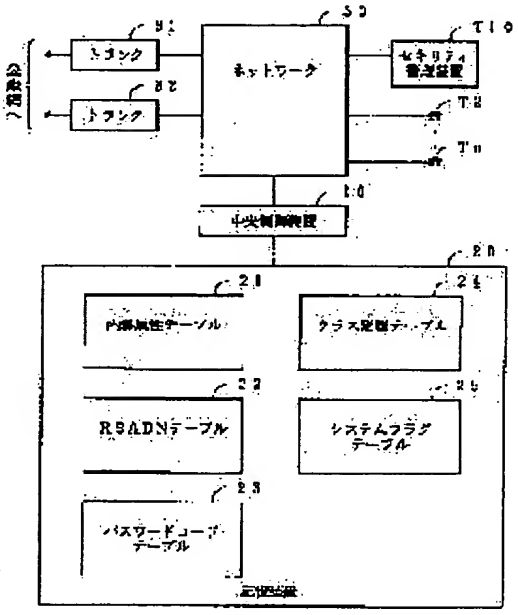
(51)Int.Cl. H04M 3/42
H04M 15/00

(21)Application number : 06-035118
(22)Date of filing : 07.03.1994

(71)Applicant : FUJITSU LTD
(72)Inventor : SUZUKI YUTAKA
MOGI UMIHIKO

(54) REMOTE SYSTEM ACCESS CONNECTION RESTRICTION METHOD

(57)Abstract:
PURPOSE: To prevent surreptitious and illicit use of a password code by connecting an incoming call to a security management equipment of a private branch electronic exchange so as to confirm an extension class of the security management equipment thereby transferring the incoming call to an extension number (DN) for a remote system access(RSA).
CONSTITUTION: An incoming call from a remote location to a trunk 31 via a public network is connected to a security management equipment T10 of a private branch exchange and a qualification of a caller itself is confirmed through the matching between an ID code of the caller itself and a code using a date/time and a random number. Then an extension class of an equipment T10 is confirmed by using a network 30, a CPU 10, and a storage device 20 or the like having an extension attribute table 21, an RSADN table 22 and a pass word code table 23 or the like and a call from the equipment T10 to the RSADN is transferred, the access to the RSA is made and the service is started. Surreptitious and illicit use of a password code are prevented by using the security management equipment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－245657

(43)公開日　平成７年(1995)９月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｍ	3/42	Ｅ			
		Ｃ			
		Ｄ			
	15/00	Ｚ			

審査請求　未請求　請求項の数11　ＯＬ　（全 14 頁）

(21)出願番号　特願平6－35118

(22)出願日　平成６年(1994)３月７日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　鈴木　豊
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　茂木　海彦
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　井桁　貞一

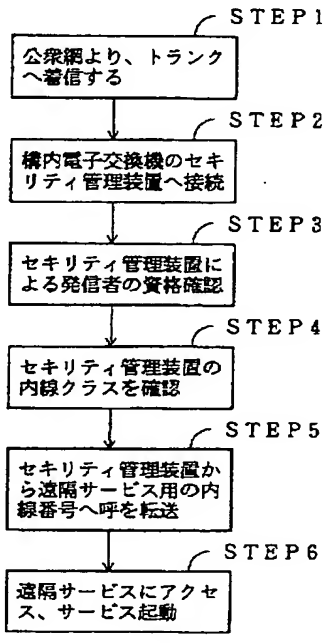
(54)【発明の名称】　遠隔システムアクセス接続規制方法

(57)【要約】

【目的】本発明は構内電子交換機の提供するサービスを公衆網から利用する際の接続規制方法に関し、パスワードコードの管理強化を可能とするセキリティ管理装置を構内電子交換機に接続し、セキリティチェックを強化することのできるＲＳＡ接続規制方法を実現することを目的とする。

【構成】ＳＴＥＰ１で発信者からの呼が公衆網より構内電子交換機のトランクに着信し、ＳＴＥＰ２でこの着信呼を構内電子交換機のセキリティ管理装置Ｔ１０に接続し、ＳＴＥＰ３でセキリティ管理装置Ｔ１０により、発信者の資格を確認する。そして、ＳＴＥＰ４ではセキリティ管理装置Ｔ１０の内線クラスを確認し、ＳＴＥＰ５でセキリティ管理装置Ｔ１０がＲＳＡＤＮに転送可能な場合は、該着信呼をＲＳＡＤＮに転送し、ＳＴＥＰ６は遠隔サービスにアクセスし、サービスを起動するように構成する。

本発明の原理を説明する図



1

【特許請求の範囲】

【請求項１】　構内電子交換機の提供するサービスを公衆網から利用する際の接続規制方法であって、

発信者からの呼が公衆網より構内電子交換機のトランクに着信し（ＳＴＥＰ１）、

次いで、該着信呼を、構内電子交換機のセキリティ管理装置（Ｔ１０）に接続し（ＳＴＥＰ２）、

前記セキリティ管理装置（Ｔ１０）により、発信者の資格の確認を行い（ＳＴＥＰ３）、

発信者の資格が遠隔システムアクセスを許可されている場合、前記セキリティ管理装置（Ｔ１０）の内線クラスを確認し（ＳＴＥＰ４）、

前記セキリティ管理装置（Ｔ１０）の内線クラスが遠隔システムアクセスサービス用の内線番号（ＲＳＡＤＮ）に転送可能な場合には、該着信呼を前記セキリティ管理装置（Ｔ１０）から遠隔システムアクセスサービス用の内線番号（ＲＳＡＤＮ）に転送し（ＳＴＥＰ５）し、

遠隔サービスにアクセスし、サービスを起動する（ＳＴＥＰ６）、

ことを特徴とする遠隔システムアクセス接続規制方法

【請求項２】　前項記載の遠隔システムアクセス接続規制方法において、

記憶装置（２０）に、構内電子交換機に収容される内線端末ごとのサービスクラスを定義する内線属性テーブル（２１）と、

前記内線属性テーブル（２１）で定義されるサービスクラスごとの接続規制内容を定義するクラス定義テーブル（２４）を設け、

遠隔システムアクセスサービス用の内線番号（ＲＳＡＤＮ）に接続を行うとき、前記内線属性テーブル（２１）に定義されたサービスクラスの接続可能サービスを前記クラス定義テーブル（２４）より索引し、遠隔システムアクセスサービス用の内線番号（ＲＳＡＤＮ）に接続を行うことにより、遠隔システムアクセスサービスにアクセス可能な呼を内線からの転送呼に限定することを特徴とする請求項１記載の遠隔システムアクセス接続規制方法。

【請求項３】　１項記載の遠隔システムアクセス接続規制方法において、

前記遠隔システムアクセスサービス用の内線番号（ＲＳＡＤＮ）にアクセスするとき、自動的に外付けの前記セキリティ管理装置（Ｔ１０）に接続するＳＴＥＰ（２０）、

を設けたことを特徴とする請求項１記載の遠隔システムアクセス接続規制方法。

【請求項４】　１項記載の遠隔システムアクセス接続規制方法において、

前記セキリティ管理装置（Ｔ１０）から、遠隔システムアクセス用の内線番号（ＲＳＡＤＮ）に転送を行うとき、パスワードコードの入力が必要であるか否かを判定

2

するステップ（ＳＴＥＰ３０）、

を設けたことを特徴とする請求項１記載の遠隔システムアクセス接続規制方法。

【請求項５】　パスワードコードの設定と、受信したパスワードコードと設定しておいたパスワードコードとを比較可能な遠隔システムアクセスサービスを提供する構内電子交換機において、

遠隔システムアクセスへのアクセスを行うとき、パスワードコードごとに遠隔システムアクセス使用回数を計数し、そのアクセス回数が許容回数を越えるか否かを判定するステップ（ＳＴＥＰ５０）を設け、

アクセス回数が許容回数を越えるか場合は以降の遠隔システムアクセスを禁止することを特徴とする遠隔システムアクセス接続規制方法。

【請求項６】　５項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、パスワードコードごとに遠隔システムアクセスで使用した料金を累積し、その使用累積料金が許容料金を越えるか否かを判定するステップ（ＳＴＥＰ６０）を設け、

アクセスの使用累積料金が許容料金を越えるか場合は以降の遠隔システムアクセスを禁止することを特徴とする請求項５記載の遠隔システムアクセス接続規制方法。

【請求項７】　５項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、遠隔システムアクセスの使用回数、および使用料金を計数する遠隔システムアクセスルーティング先を指定することを特徴とする請求項５記載の遠隔システムアクセス接続規制方法。

【請求項８】　パスワードコードの設定、比較と、録音装置（Ｔ２０）へのルーティングが可能な遠隔システムアクセスサービスを提供する構内電子交換機において、

遠隔システムアクセスへのアクセスを行うとき、ＲＳＡ接続先スクリーニングテーブル（２８）を照合し、前記ＲＳＡ接続先スクリーニングテーブル（２８）に指定される特定の遠隔システムアクセス先番号がダイヤルされた場合は前記録音装置（Ｔ２０）に接続するステップ（ＳＴＥＰ７０）、を設けたことを特徴とする遠隔システムアクセス接続規制方法。

【請求項９】　８項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、ＲＳＡ接続先スクリーニングテーブル（２８）を照合し、前記録音装置（Ｔ２０）への接続を行った際、システム管理用の多機能電話機（Ｔ３０）に前記録音装置（Ｔ２０）にルーティングされたことを通知するステップ（ＳＴＥＰ８０）、を設けたことを特徴とする請求項８記載の遠隔システムアクセス接続規制方法。

【請求項１０】　８項記載の遠隔システムアクセス接続

規制方法において、
遠隔システムアクセスへのアクセスを行うとき、ＲＳＡ接続先スクリーニングテーブル（２８）を照合し、前記録音装置（Ｔ２０）への接続を行った際、システム管理用の前記多機能電話機（Ｔ３０）に前記録音装置（Ｔ２０）にルーティングされたことを通知し、前記録音装置（Ｔ２０）の録音内容から遠隔システムアクセスに使用されたパスワードコードを再生するステップ（ＳＴＥＰ９０）、を設けたことを特徴とする請求項８記載の遠隔システムアクセス接続規制方法。

【請求項１１】　８項記載の遠隔システムアクセス接続規制方法において、
遠隔システムアクセスへのアクセスを行うとき、ＲＳＡ接続先スクリーニングテーブル（２８）を照合し、前記録音装置（Ｔ２０）への接続を行い、該録音内容の再生により、不正使用と判定したときは、パスワードコードを無効とすることを特徴とする請求項８記載の遠隔システムアクセス接続規制方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は構内電子交換機の提供するサービスを公衆網から利用する際の接続規制方法に関する。

【０００２】電子交換機の技術の進展に伴い、構内電子交換機は単に構内電子交換機に収容された電話機相互間の通話のための交換接続を行うのみではなく、例えば、メールサービス、会議電話等の各種のサービスを提供するようになってきている。

【０００３】このような構内電子交換機が提供するサービスを遠隔地にいる発信者が公衆網を通してサービスを利用する遠隔システムアクセス（Remote System Access、以下ＲＳＡと称する）サービスが普及してきている。このサービスは、例えば、在宅勤務者や出張者等社外にいる発信者が自宅の電話や公衆電話から会社の構内電子交換機にアクセスし、この構内電子交換機の提供するサービスである会議通話、公衆網発信や音声メール等を利用するものである。

【０００４】かかるＲＳＡサービスにおいて、パスワードコードの盗用、悪用を防止することのできるＲＳＡ接続規制方法が要求されている。

【０００５】

【従来の技術】図１３は従来例の構内電子交換システムを説明する図を示す。図中の１０は中央制御装置であり、２０は記憶装置であり、３０はネットワークであり、３１、３２は公衆網に接続されるトランクであり、Ｔ１～Ｔｎは端末である。

【０００６】また、記憶装置２０の中の２２はＲＳＡを利用するための内線番号群としてのＲＳＡＤＮテーブルであり、２３はパスワードコードテーブルであり、パスワードコードごとに接続可能なＲＳＡサービスが定義されている。

【０００７】図１４は従来例のフローチャートである。以下フローチャートにしたがって、接続動作を説明する。ＳＴＥＰ（以下ｓと略称する）１１；遠隔地にいる発信者からの呼が、公衆網を経由して構内電子交換機のトランク３１に着信し、構内電子交換機は受信したダイヤルを分析する。

【０００８】ｓ１２；着信先がＲＳＡサービスへの接続を行うために設けられた内線Ａであるか否かを判定する。ここでは、端末Ｔ１が内線Ａであるものとし、以下内線Ａと称する。

【０００９】ｓ１３；公衆網を経由する発信者と内線Ａが接続される。

ｓ１４；内線Ａがフッキングを行い、ＲＳＡＤＮをダイヤルすると、内線Ａにはダイヤルトーン（図中はＤＴと称する）が接続される。

【００１０】ｓ１５；内線Ａがオンフックする。

ｓ１６；内線Ａのオンフックにより、トランク３１にダイヤルトーンが送出され、発信者から送出されるパスワードコード（図中ＰＷＣと略称する）を受信する。

【００１１】ｓ１７；パスワードコードがパスワードコードテーブル２３に登録されているパスワードコードに一致するか否かを判定する。

ｓ１８；パスワードコードに一致した場合には、構内電子交換機のサービスの提供が可能であり、発信呼のクラスをパスワードコードのクラスに変更する。

【００１２】ｓ１９；トランク３１にダイヤルトーンを送出する。

ｓ１９ａ；発信者が送出するダイヤルを受信する。

ｓ１９ｂ；指定されたサービスを起動する。

【００１３】ｓ１２ａ；ｓ１２で着信先が内線Ａでない場合、さらにＲＳＡＤＮへの着信であるか否かを判定し、ＲＳＡＤＮへの着信の場合には、ｓ１５へ進む。

ｓ１２ｂ；着信先が内線Ａでなく、ＲＳＡＤＮでもない場合は、通常の着信であるので通常の着信処理を行う。

【００１４】ｓ１７ａ；ｓ１７でパスワードコードが一致しない場合は、ＲＳＡへの接続を行わずＲＯＴ(Reorder Tone)接続を行う。

以上のような接続処理により、公衆網を経由した発信者が恰も構内電子交換機に収容されている端末Ｔ1 ～Ｔｎと同等の状態におかれ、ＲＳＡサービスを受けることができる。

【００１５】

【発明が解決しようとする課題】上述の従来例において、ＲＳＡサービス接続の可否を判定するのは、パスワードコードの照合のみであり、ＲＳＡサービスを利用するためのパスワードコードが盗用あるいは悪用された場合、公衆網－専用線－公衆網接続や公衆網－公衆網接続が許容されている環境においては、長距離通話や国際通話が不当に行われてしまい、構内電子交換機を所有して

5

いる会社に膨大な通話料金の支払いが請求されることがある。

【００１６】本発明は、パスワードコードの管理強化を可能とするセキリティ管理装置を構内電子交換機に接続し、セキリティチェックを強化することのできるＲＳＡ接続規制方法を実現しようとする。

【００１７】

【課題を解決するための手段】図１は本発明の原理を説明する図である。図はＲＳＡ接続規制方法を示し、ＳＴＥＰ１で発信者からの呼が公衆網より構内電子交換機のトランクに着信し、ＳＴＥＰ２で該着信呼を、構内電子交換機のセキリティ管理装置Ｔ１０に接続し、ＳＴＥＰ３でセキリティ管理装置Ｔ１０により、発信者の資格の確認を行う。

【００１８】さらに、ＳＴＥＰ４で発信者の資格が遠隔システムアクセスを許可されている場合、セキリティ管理装置Ｔ１０の内線クラスを確認し、ＳＴＥＰ５でセキリティ管理装置Ｔ１０の内線クラスが遠隔システムアクセスサービス用の内線番号ＲＳＡＤＮに転送可能な場合には、該着信呼をセキリティ管理装置Ｔ１０から遠隔システムアクセスサービス用の内線番号ＲＳＡＤＮに転送し、ＳＴＥＰ６で遠隔サービスにアクセスし、サービスを起動する。

【００１９】

【作用】公衆網を経由する発信者が構内電子交換機の提供する各種のサービスを利用するとき、公衆網から構内電子交換機のトランクに着信させた後、セキリティ管理装置Ｔ１０に接続する。この状態で発信者とセキリティ管理装置Ｔ１０が接続され、セキリティ管理装置Ｔ１０で、日時、乱数等により個人ＩＤコードのチェックを厳重に行う。例えば、日時をキーとして乱数を発生する同じ乱数発生器を発信者、セキリティ管理装置Ｔ１０が持っており、発信者から送られてきた乱数がセキリティ管理装置Ｔ１０で発生した乱数と一致することを確認する。このようにして、公衆網を経由する発信者の資格はセキリティ管理装置Ｔ１０で厳重にチェックされた後、ＲＳＡＤＮへ転送しサービスを起動する。

【００２０】このように、ＲＳＡＤＮへアクセスできる発信者はセキリティ管理装置Ｔ１０の厳重なる資格チェックで許可となった者のみであり、ＲＳＡへの不法なアクセスを防止することができる。

【００２１】また、構内電子交換機に登録したパスワードコードごとに使用料金、使用回数を監視することにより、パスワードの盗用、悪用を防ぐことができる。さらに、特定のＲＳＡアクセス番号がダイヤルされた場合、録音装置Ｔ２０へのルーティングを可能にしておき、録音装置Ｔ２０の録音内容から使用されたパスワードコードを確認することにより、パスワードの盗用、悪用を防ぐことができる。

【００２２】

6

【実施例】図２は本発明の実施例の構内電子交換システム（１）を説明する図である。図中の１０は交換処理を制御する中央制御装置であり、２０は交換処理プログラム、各種テーブルを記憶する記憶装置、３０は指定の端末相互間の接続を行うネットワークである。

【００２３】また、３１、３２はトランクであり、Ｔ１０は内線Ａとして接続されるセキリティ管理装置、Ｔ２～Ｔｎは端末である。本発明において、記憶装置２０には、内線のクラス属性を定義する内線属性テーブル２１、ＲＳＡサービスを利用するための内線番号群としてのＲＳＡＤＮテーブル２２、発信者の資格を確認するためのパスワードコードテーブル２３、サービスクラスごとに利用可能なサービスを定義するクラス定義テーブル２４、各種システムフラグを定義するシステムフラグテーブル２５が設けられている。

【００２４】図３は本発明の実施例のテーブル構成（１）を説明する図である。（Ａ）は内線属性テーブル２１の構成を示し、各内線ごとにサービスクラス（Class Of Service、以下ＣＯＳと略称する）、接続規制クラス（Restriction Mode、以下ＲＳＭと略称する）、ファシリティ規制クラス（Facility Restriction Level、以下ＦＲＬと略称する）の値が定義され、（Ｂ）はＲＳＡＤＮテーブル２２の構成を示し、各ＲＳＡＤＮごとにサービスクラスＣＯＳ、接続規制クラスＲＳＭ、ファシリティ規制クラスＦＲＬおよびセキリティグループ番号（Security Group、以下ＳＧＲＰと略称する）の値が定義されている。このセキリティグループ番号（ＳＧＲＰ）は番号ごとにセキリティ用のパスワードコード群を定義するための管理番号である。

【００２５】また、（Ｃ）はパスワードコードテーブル２３の構成を示し、パスワードコード（Pass Word Code、以下ＰＷＣと略称する）、およびパスワードコードＰＷＣとしてのサービスクラスＣＯＳ、接続規制クラスＲＳＭ、ファシリティ規制クラスＦＲＬの値が定義され、（Ｄ）はクラス定義テーブル２４の構成を示し、サービスクラＣＯＳごとにどのサービスが可能であるかを定義し、（Ｅ）はシステムフラグテーブル２５の構成を示し、ＲＳＡサービスへの直接アクセス許容フラグ２５１、セキリティ管理装置Ｔ１０への自動迂回フラグ２５２およびパスワードコード省略フラグ２５３が格納されている。

【００２６】図４は本発明の実施例のフローチャート（１）を示す。図は請求項１、２に対応する実施例のフローチャートであり、以下フローチャートにより本発明の動作を説明する。

【００２７】ＳＴＥＰ（以下Ｓと略称する）１１；遠隔地にいる発信者からの呼が公衆網を経由して構内電子交換機のトランク３１に着信し、構内電子交換機は受信したダイヤルを分析する。

【００２８】Ｓ１２；着信先がＲＳＡサービスを行うた

めに設けられた内線Ａであるか否かを判定する。ここでは、内線Ａに外付けのセキリティ管理装置Ｔ１０が接続されているものとする。

【００２９】Ｓ１３；公衆網を経由する発信者とセキリティ管理装置（図中はセキリティ装置と略称する）Ｔ１０が接続され、自動応答し二者通話状態となる。このとき、セキリティ管理装置Ｔ１０から発信者へＩＤコード等を入力することを指示するメッセージを送出し、セキリティ管理装置Ｔ１０は発信者からのＩＤコード等を受信し、一連の資格チェックを行う。

【００３０】Ｓ１４；セキリティ管理装置Ｔ１０による資格チェックの結果、正当な利用者と判断した場合は、セキリティ管理装置Ｔ１０はフッキングを行い、ＲＳＡサービス専用の電話番号ＲＳＡＤＮを送出する。

【００３１】Ｓ１５；中央制御装置１０は転送先がＲＳＡＤＮであることから、内線Ａのサービスクラスを内線属性テーブル２１から読み出し（ここではＣＯＳ＝０）、クラス定義テーブル２４のＲＳＡ転送が許容されているか否かを判定し、許容されていない場合にはＳ１５ａへ進む。

【００３２】Ｓ１６；ＲＳＡ転送が許容されている場合には、発信呼のクラス属性を一時的に内線Ａのクラス属性に置き換える。

Ｓ１７；ＲＳＡＤＮへ仮想的に接続され、ダイヤルトーン（図中ＤＴと示す）を接続し、内線Ａをオンフックする。

【００３３】Ｓ１８；内線Ａがオンフックすることにより、トランク３１とＲＳＡＤＮとが仮想的に接続され発信者はダイヤルトーンを聴取する。

Ｓ１９；ダイヤルトーンを聴取し、発信者は希望するサービスにアクセスするコード、あるいは、公衆網に発信する場合は、公衆網に発信するアクセスコードおよび相手先番号をダイヤルする。

【００３４】Ｓ１９ａ；中央制御装置１０は指定のサービスの起動あるいは公衆網に接続するためにトランク３２を起動し接続動作を行う。

Ｓ１２ａ；Ｓ１２で着信先が内線Ａでない場合は通常の着信であるので通常の着信処理を行う。

【００３５】Ｓ１５ａ；Ｓ１５でＲＳＡへの転送を許可されていない場合は、ＲＳＡへの接続を行わずＲＯＴ接続を行う。

このような手順により、公衆網を経由しＲＳＡサービスへアクセスする発信者の資格をセキリティ管理装置Ｔ１０で確実にチェックすることにより、不法なアクセスを防止することができる。さらに、ＲＳＡＤＮへの転送を行うとき、該内線のサービスクラスをクラス定義テーブル２４を参照し、転送が許容されている内線であるか否かを判定することにより、ＲＳＡＤＮへの転送可能とする内線を限定することができる。

【００３６】図５は本発明の実施例のフローチャート

（２）を示す。図は請求項３、４に対応する実施例のフローチャートであり、ＲＳＡＤＮに直接着信してきた場合、自動的に外付けのセキリティ管理装置Ｔ１０に接続するためのステップ２０としてのＳ２１～Ｓ２３、およびＲＳＡＤＮに転送するときパスワードコードの入力が必要か否かを判定するステップ３０としてのＳ３１～Ｓ３５を設けたものである。以下フローチャートにより動作を説明する。

【００３７】Ｓ１１；発信者からの呼が構内電子交換機のトランク３１に着信し、受信したダイヤルを分析する。

Ｓ１２；着信先がＲＳＡサービスを行うために設けられた内線Ａであるか否かを判定する。ここでは、内線Ａへの着信でない場合はＳ２１へ進む。

【００３８】Ｓ２１；内線Ａへの着信でない場合、次いで、ＲＳＡＤＮへの着信か否かを判定し、ＲＳＡＤＮへの着信でない場合、Ｓ１３ａへ進む。

Ｓ２２；さらに、システムフラグテーブル２５を参照して、ＲＳＡへの直接アクセス許容フラグ２５１が立っているか否かを判定し、立っていない場合はＳ１５ａへ進む。

【００３９】Ｓ２３；システムフラグテーブル２５を参照して、セキリティ管理装置Ｔ１０への自動迂回フラグ２５２が立っているか否かを判定し、立っていない場合はＳ１３へ進む。

【００４０】Ｓ１３～Ｓ１７；着信先が内線Ａの場合、セキリティ管理装置Ｔ１０が接続され、セキリティ管理装置Ｔ１０は発信者からのＩＤコード等を受信し、一連の資格チェックを行った上でＲＳＡサービス専用の電話番号ＲＳＡＤＮを送出し、内線Ａのサービスクラスが許容されているか否かを判定し、許容されている場合には、発信呼のクラス属性を一時的に内線Ａのクラス属性に置き換える。

【００４１】Ｓ３１；システムフラグテーブル２５を参照して、パスワードコード省略フラグ２５３が立っているか否かを判定し、省略可の場合にはＳ１８へ進む。

Ｓ３２；パスワードコードの入力を省略できない場合は、トランク３１にダイヤルトーンを接続し、パスワードコードの入力を指示する。

【００４２】Ｓ３３；発信者からのパスワードコードを受信する。

Ｓ３４；中央制御装置１０は受信したパスワードコードがＲＳＡＤＮテーブル２２に格納されているパスワードコード群の中のものと一致するか否かを判定し一致しない場合はＳ１５ａに進む。

【００４３】Ｓ３５；パスワードコードが一致した場合は、発信呼のクラスをパスワードコードのクラスに変更し、Ｓ１８へ進む。

Ｓ１８～Ｓ１９ａ；発信者は希望するサービスにアクセスするコードを入力することにより、サービスを起動す

る。

【００４４】このような手順により、内線転送呼以外の呼がＲＳＡＤＮにアクセスしようとするとき、自動的に外付けのセキリティ管理装置Ｔ１０が接続されている内線Ａにルーティングするとともに、ＲＳＡＤＮにアクセス可能な呼を内線からの転送呼に限定することができる。

【００４５】また、本実施例においては、外付けのセキリティ管理装置Ｔ１０において、厳重なる資格チェックが可能であるので、パスワードコードの入力をスキップし、指定のＲＳＡサービスへアクセスすることができる。

【００４６】図６は本発明の実施例の構内電子交換システム（２）を説明する図である。図は図２で説明した構内電子交換システム（１）の中央制御装置１０に、各種テーブルのデータを設定するデータ設定部１１、各種接続動作の回数をカウントするカウンタ１２、データ接続部１１で設定した値とカウンタ１２によるカウント値を比較するデータ比較部１３、詳細課金情報制御部１０Ａとのインタワークを行う課金情報インタワーク部（図中課金情報ＩＮＴと称する）１４を設け、記憶装置２０には各種データを設定するデータテーブル２６を設けたものである。

【００４７】図７は本発明の実施例のデータテーブルを説明する図である。データ設定部１１によりデータテーブル２６の中にパスワードコードごとに次のデータを設定する。

【００４８】　ルーティング先番号ごとの局線トランク発信許容回数。

　ルーティング先番号ごとの局線トランク発信使用回数。

　ルーティング先番号ごとの専用線トランク発信許容回数。

【００４９】　ルーティング先番号ごとの専用線トランク発信使用回数。

　、　を含むＲＳＡアクセスから利用可能な構内電子交換機のサービスへアクセス可能な許容回数。

【００５０】　、　を含むＲＳＡアクセスから利用可能な構内電子交換機のサービスへアクセスした回数。

　におけるサービスアクセスの累積使用料金の上限。

【００５１】　におけるサービスアクセスの実際に使用した料金の累計。図８は本発明の実施例のフローチャート（３）を示す。図は請求項５、６に対応する実施例のフローチャートであり、ＳＴＥＰ５０とＳＴＥＰ６０としてのＳＴ６０′～ＳＴ６４を設けたものであり、以下フローチャートにより本発明の動作を説明する。

【００５２】Ｓ５０；ＲＳＡへアクセスを行うとき、データテーブル２６の中のパスワードコードごとのＲＳＡサービス（図中はＲＳＡＳと示す）トータルアクセス使

用回数　がトータルアクセス許容回数　未満か否かを判定し、許容回数を越えた場合はＳ６４に進む。

【００５３】Ｓ６０′；さらに、データテーブル２６の中のパスワードコードごとのサービスアクセスに使用した料金の累計　がアクセスの累積使用料金の上限　未満か否かを判定し、使用料金の上限を越えた場合はＳ６４に進む。

【００５４】Ｓ６０ａ；アクセスするＲＳＡサービスは局線発信／専用線発信の何れかであるか否かを判定し、否の場合にはＳ６１へ進む。

Ｓ６０ｂ；ＲＳＡルーティング先番号はデータテーブル２６の中に登録されているか否かを判定し、否の場合にはＳ６４に進む。

【００５５】Ｓ６０ｃ；ＲＳＡルーティング先番号のデータテーブル２６の中の発信使用回数　は許容回数　以下か否かを判定し、否の場合にはＳ６４に進む。

Ｓ６１；許容の場合にはデータテーブル２６の使用したルーティング先番号の使用回数を「＋１」カウントする。

【００５６】Ｓ６２；ＲＳＡサービスへのトータルアクセス回数を「＋１」カウントする。

Ｓ６３；サービス終了後、ＲＳＡサービスの使用料金を累積する。

Ｓ６４；該サービスをブロックとし、アクセスしてきた発信者に対して、トーン、アナウンス等によりブロックとしたことを通知する。

【００５７】Ｓ６０ｃで、ルーティング先番号ごとに使用回数を許容回数と比較し、使用可否を決めているが、ルーティング先番号ごとに使用料金の累計を累積使用料金の上限と比較し、使用可否を決めることも可能である。

【００５８】また、図７のデータテーブルのようにテーブルを構成することにより、遠隔システムアクセスのルーティング先を任意に設定することができる。例えば、「０３」と指定すれば、「０３」で始まるすべての番号をルーティング先として指定することが可能となる。

（請求項７対応）

図９は本発明の実施例の構内電子交換システム（３）を説明する図である。図は図２で説明したＲＳＡＤＮテーブル２２、パスワードコードテーブル２３を備える記憶装置２０に、表示機能付き多機能電話機Ｔ３０のボタン情報を管理する多機能電話ボタンテーブル２７、ＲＳＡアクセス呼を録音装置Ｔ２０にルーティングする宛先呼を格納したＲＳＡ接続先スクリーニングテーブル２８、特定の発信者からの呼以外を自動的に録音装置Ｔ２０にルーティングさせるための発信者番号を定義した発信者スクリーニングテーブル２８Ａ、メッセージ番号、使用フラグ等を書き込むＲＳＡ録音メッセージテーブル２９を設け、ネットワーク３０には録音装置Ｔ２０、システム管理者用の表示機能付き多機能電話機Ｔ３０を接続し

たものである。

【００５９】図１０は本発明の実施例のテーブル構成（２）を説明する図である。ＲＳＡＤＮテーブル２２、パスワードコードテーブル２３は図３と説明したと同じ内容であるので説明は省略する。

【００６０】（Ａ）は多機能電話機ボタンテーブル２７の構成を示し、各多機能電話機の内線ごとに実装されているボタンの機能が定義されている。例えば、ここでは、多機能電話機Ｔ３０は構内電子交換機の内線Ｂに接続されており、そのボタン００は主回線に、ボタン０２はＲＳＡ管理に割り当てられている。（Ｂ）はＲＳＡ接続先スクリーニングテーブル２８の構成を示し、ＲＳＡアクセス呼を録音装置Ｔ２０に接続するべき宛先コードが格納されており、このテーブルに定義された宛先番号がトランク３１から受信された場合には録音装置Ｔ２０に自動的に接続する。

【００６１】また、（Ｃ）は発信者スクリーニングテーブル２８Ａの構成を示し、自動ルーティングを行わない発信者番号群が格納されており、（Ｄ）はＲＳＡ録音メッセージテーブル２９の構成を示し、メッセージ番号、使用中フラグ（０；未使用、１；使用中）、パスワードコード（ＰＷＣ）、ダイヤルされた番号、呼が発生した日時および再生フラグ（０；未再生、１；再生済）が書き込まれる。

【００６２】図１１は本発明の実施例のフローチャート（４）を示す。図は請求項８、９に対応する実施例のフローチャートであり、ＲＳＡ呼が着信したときの処理フローチャートであり、ＳＴＥＰ７０としてのＳＴ７１～ＳＴ７８とＳＴＥＰ８０を設けたものである。以下フローチャートにより本発明の動作を説明する。

【００６３】Ｓ１１～Ｓ１９；トランク３１へ着信し、ダイヤル受信した数字がＲＳＡＤＮテーブル２２内に格納されているコードのどれかと一致した場合、ＲＳＡＤＮへ仮想的に接続されＤＴが送出される。発信者はパスワードコードを入力し、パスワードコードが一致した場合、さらにサービスにアクセスするコードまたは公衆網に発信するアクセスコードと相手先番号をダイヤルすることでトランク３２を起動し接続が完了する動作は図５のフローチャートで説明したのと同じ動作である。

【００６４】Ｓ７１；受信したアクセスコードがトランクにアクセスするコードか否かを判定し、否の場合にはＳ７１ａへ進む。

Ｓ７２；ＲＳＡ接続先スクリーニングテーブル２８を検索する。

【００６５】Ｓ７３；受信した宛先コードがＲＳＡ接続先スクリーニングテーブル２８の内容と一致しない場合はＳ１９ａに進む。

Ｓ７４；受信したコードが本テーブル内に格納されている宛先コードと一致する場合は、この呼を録音装置Ｔ２０に接続し、使用中フラグが「０」であるメッセージ番号を探し、該メッセージ番号に使用中フラグ「１」を立てる。

【００６６】Ｓ７５；発信者に対し予め決められた合言葉の入力を促すためのトーンあるいはアナウンスを送出する。

Ｓ７６；トランク３１をメッセージ番号に対応する録音ポートに一定時間接続する。

【００６７】Ｓ７７；ＲＳＡ録音メッセージテーブル（図中ＲＳＡ録音テーブルと略称する）２９に受信したパスワードコード、宛先番号、現在日時情報を格納する。

Ｓ７８；一定時間経過後に録音ポートを解放し、その旨を示すトーンあるいはアナウンスを送出する。

【００６８】Ｓ８０；多機能電話Ｔ３０のＲＳＡ管理ボタンに対応するボタンのランプを点滅させることで、システム管理者に録音装置Ｔ２０経由で発信したＲＳＡ呼が発生し、メッセージが残されたことを通知する。

【００６９】図１２は本発明の実施例のフローチャート（５）を示す。図は請求項１０、１１に対応する実施例のフローチャートであり、録音装置Ｔ２０の録音内容を再生する処理フローチャートであり、ＳＴＥＰ９０としてのＳＴ９１～ＳＴ９９を設けたものである。以下フローチャートにより本発明の動作を説明する。

【００７０】Ｓ８０；多機能電話機Ｔ３０のＲＳＡ管理ボタンのランプ点滅（図１１のＳ８０に同じ）。

Ｓ９１；多機能電話機Ｔ３０のＲＳＡ管理ボタンを押下げる。

【００７１】Ｓ９２；多機能電話機Ｔ３０と録音装置Ｔ２０が接続される。

Ｓ９３；多機能電話機Ｔ３０に使用フラグ「１」、再生フラグ「０」の未再生のメッセージ番号に対応する録音メッセージの内容を送出し、多機能電話機Ｔ３０の表示部に該メッセージ番号に対応するパスワード呼、宛先番号および日時を表示する。

【００７２】Ｓ９４；一定時間後に録音ポートを解放し、その旨を示すトーンあるいはアナウンスを送出する。

Ｓ９５；多機能電話機Ｔ３０のダイヤルにより次の選択が可能となる。

【００７３】Ｓ９５ａ；メッセージ内容が正当か否かの判定を保留し、後で確認する場合。

＊を入力する。本メッセージは未再生のまま残される。メッセージ番号対応の使用中フラグ「１」、再生フラグ「０」と設定する。

【００７４】Ｓ９５ｂ；メッセージ内容が正当な場合。

＃を入力する。本メッセージはクリアされ、メッセージ番号対応の使用中フラグ「０」、再生フラグ「０」と設定する。

【００７５】Ｓ９５ｃ；メッセージ内容が不当な場合。

９９を入力する。本メッセージはクリアされ、メッセー

ジ番号対応の使用中フラグ「０」、再生フラグ「０」と設定する。

【００７６】Ｓ９６；このとき、該当のパスワードコードは盗用または悪用されたものと判定し、パスワードコードテーブル２３より削除する。

９５ｄ；上記コードを入力せずに多機能電話機Ｔ３０を切断した場合は、９５ａが設定されたものとして処理する。

【００７７】Ｓ９７；未再生メッセージが有るか否かを判定し、存在している場合は９２に戻る。

Ｓ９８；未再生メッセージがない場合には終了トーンを送出する。

【００７８】Ｓ９９；切断を行う。

上述の処理によりパスワードコードの悪用、盗用を防止することができる。

【００７９】

【発明の効果】本発明によれば、構内電子交換機が提供する各種サービスを公衆網から利用するＲＳＡサービスにおいて、セキリティ装置との連携を行い、セキリティ装置を経由した呼のみにＲＳＡ接続を許容することにより、セキリティチェックを強化することができる。

【００８０】また、パスワードコードごとに利用上限を設定し、上限を超えない範囲でＲＳＡサービスの利用を許容することで、膨大な料金の不法アクセスを制限することができる。

【００８１】さらに、特定宛先に発信する呼や不特定の発信元からの呼に対しては音声による合言葉を録音し、確認することにより正当性を確実にチェックすることが可能となる。

【図面の簡単な説明】

【図１】　本発明の原理を説明する図

【図２】　本発明の実施例の構内電子交換システム（１）を説明する図

【図３】　本発明の実施例のテーブル構成（１）を説明する図

【図４】　本発明の実施例のフローチャート（１）

【図５】　本発明の実施例のフローチャート（２）

【図６】　本発明の実施例の構内電子交換システム

（２）を説明する図

【図７】　本発明の実施例のデータテーブルを説明する図

【図８】　本発明の実施例のフローチャート（３）

【図９】　本発明の実施例の構内電子交換システム（３）を説明する図

【図１０】　本発明の実施例のテーブル構成（２）を説明する図

【図１１】　本発明の実施例のフローチャート（４）

【図１２】　本発明の実施例のフローチャート（５）

【図１３】　従来例の構内電子交換システムを説明する図

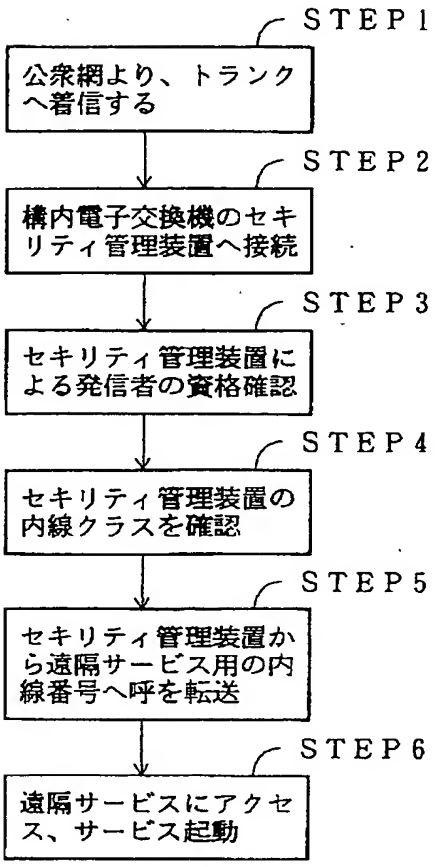
【図１４】　従来例のフローチャート

【符号の説明】

１０　中央制御装置
１１　データ設定部
１２　カウンタ
１３　データ比較部
１４　課金情報インタワーク部
１０Ａ　詳細課金情報制御部
２０　記憶装置
２１　内線属性テーブル
２２　ＲＳＡＤＮテーブル
２３　パスワードコードテーブル
２４　クラス定義テーブル
２５　システムフラグテーブル
２６　データテーブル
２７　多機能電話ボタンテーブル
２８　ＲＳＡ接続先スクリーニングテーブル
２８Ａ　発信者スクリーニングテーブル
２９　ＲＳＡ録音メッセージテーブル
３０　ネットワーク
３１、３２　トランク
Ｔ１０　セキリティ管理装置
Ｔ２０　録音装置
Ｔ３０　多機能電話機
Ｔ１～Ｔｎ　端末

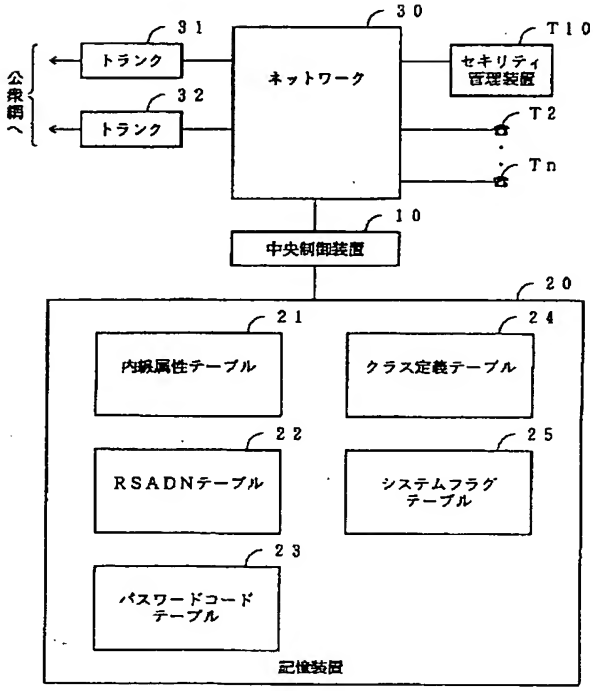
【図１】

本発明の原理を説明する図



【図２】

本発明の実施例の　内電子交換システム（１）を説明する図



【図３】

本発明の実施例のテーブル構成（１）を説明する図

(A)

21

	COS	RSM	FRL	・・・・・
内線A	0	1	6	・
内線B	1	5	0	・
・	・	・	・	・
・	・	・	・	・

(B)

22

RSADN	COS	RSM	FRL	SGRP
4000	2	3	3	1
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

(C)

23

PWC	COS	RSM	FRL
1087	3	1	6
・	・	・	・
・	・	・	・
・	・	・	・
・	・	・	・

(D)

24

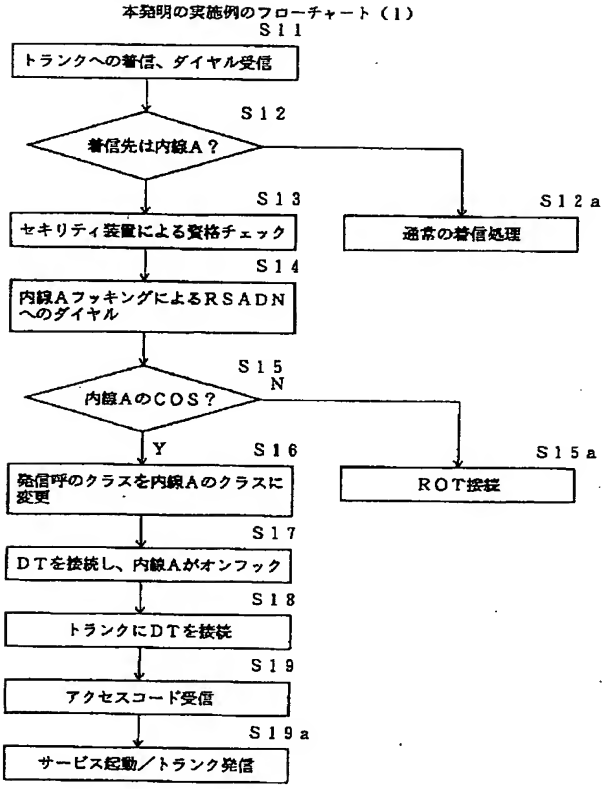
ｲﾝｷｮｺｽ	0	1	2	
RSA転送	1	0	0	

(E)

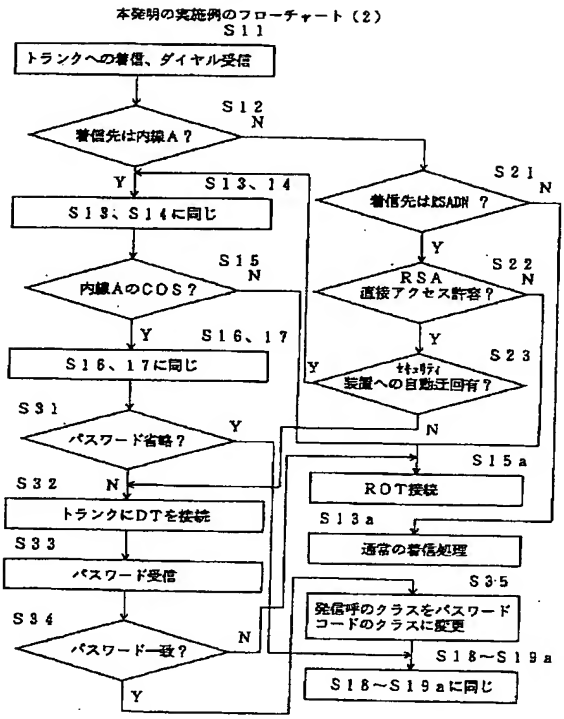
25

RSA への直接ｱｸｾｽ許容ﾌﾗｸﾞ 251	0
ｾｷｭﾘﾃｨ装置への自動迂回ﾌﾗｸﾞ 252	1
ﾊﾟｽﾜｰﾄﾞｺｰﾄﾞ省略ﾌﾗｸﾞ 253	1
・	・

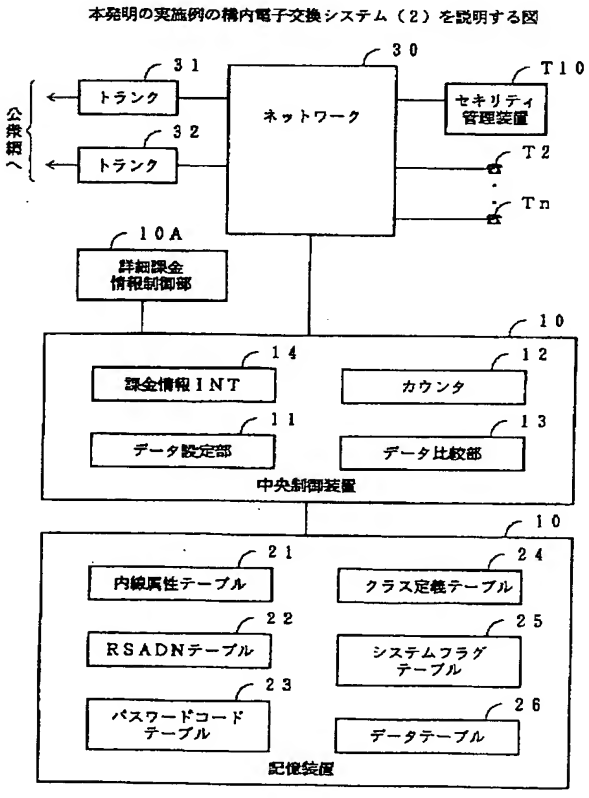
【図４】


本発明の実施例のフローチャート（１）
Ｓ１１
トランクへの着信、ダイヤル受信
Ｓ１２
着信先は内線Ａ？
Ｓ１２ａ
通常の着信処理
Ｓ１３
セキュリティ装置による資格チェック
Ｓ１４
内線Ａフッキングによる RSADN へのダイヤル
Ｓ１５
内線ＡのＣＯＳ？
Ｎ
Ｓ１５ａ
ＲＯＴ接続
Ｙ
Ｓ１６
発信呼のクラスを内線Ａのクラスに変更
Ｓ１７
ＤＴを接続し、内線Ａがオンフック
Ｓ１８
トランクにＤＴを接続
Ｓ１９
アクセスコード受信
Ｓ１９ａ
サービス起動／トランク発信

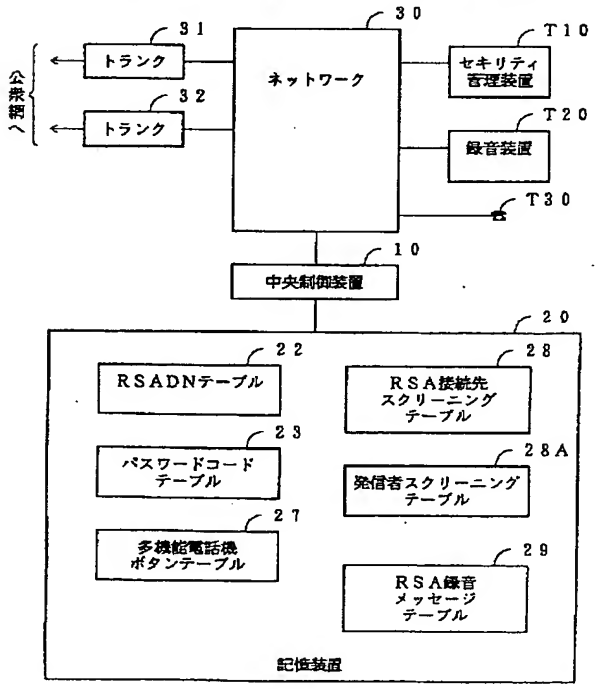
【図５】


本発明の実施例のフローチャート（２）
Ｓ１１
トランクへの着信、ダイヤル受信
Ｓ１２
着信先は内線Ａ？
Ｎ
Ｙ
Ｓ１３、１４
Ｓ１３、Ｓ１４に同じ
Ｓ１５
内線ＡのＣＯＳ？
Ｎ
Ｙ
Ｓ１６、１７
Ｓ１６、１７に同じ
Ｓ３１
パスワード省略？
Ｙ
Ｎ
Ｓ３２
トランクにＤＴを接続
Ｓ３３
パスワード受信
Ｓ３４
パスワード一致？
Ｎ
Ｙ
Ｓ２１
着信先はISADN ？
Ｎ
Ｙ
Ｓ２２
ＲＳＡ直接アクセス許容？
Ｎ
Ｙ
Ｓ２３
セキュリティ装置への自動迂回有？
Ｙ
Ｎ
Ｓ１５ａ
ＲＯＴ接続
Ｓ１３ａ
通常の着信処理
Ｓ３５
発信呼のクラスをパスワードコードのクラスに変更
Ｓ１８～Ｓ１９ａ
Ｓ１８～Ｓ１９ａに同じ

【図６】


本発明の実施例の構内電子交換システム（２）を説明する図
公衆網へ
３１
トランク
３２
トランク
３０
ネットワーク
Ｔ１０
セキュリティ管理装置
Ｔ２
Ｔｎ
１０Ａ
詳細課金情報制御部
１０
１４
課金情報ＩＮＴ
１２
カウンタ
１１
データ設定部
１３
データ比較部
中央制御装置
１０
２１
内線属性テーブル
２４
クラス定義テーブル
２２
RSADNテーブル
２５
システムフラグテーブル
２３
パスワードコードテーブル
２６
データテーブル
記憶装置

【図９】


本発明の実施例の構内電子交換システム（３）を説明する図
公衆網へ
３１
トランク
３２
トランク
３０
ネットワーク
Ｔ１０
セキュリティ管理装置
Ｔ２０
録音装置
Ｔ３０
１０
中央制御装置
２０
２２
RSADNテーブル
２８
ＲＳＡ接続先スクリーニングテーブル
２３
パスワードコードテーブル
２８Ａ
発信者スクリーニングテーブル
２７
多機能電話機ボタンテーブル
２９
ＲＳＡ録音メッセージテーブル
記憶装置

【図７】

本発明の実施例のデータテーブルを説明する図

26

パスワードコード		局線トランク発信回数		専用線トランク発信回数		RSAサービスへのトータルアクセス回数	RSAの使用累積料金
		ルーティング先番号	回数	ルーティング先番号	回数		
12345	許容回数／料金	03 044 0457771111 ①	5 5 3	4 3 74 70001234 79305678 ③	20 10 10 5 5	150 ⑤	30,000 ⑦
	使用回数／料金	03 044 0457771111 ②	3 2 2	4 3 74 70001234 79305678 ④	11 6 3 1 2	61 ⑥	6,420 ⑧
98765	許容回数／料金	0 7 ①	5 5	7 4 3 2 ③	6 6 6 2	50 ⑤	12,000 ⑦
	使用回数／料金	0 ②	4	7 4 2 ④	3 4 2	18 ⑥	4,310 ⑧

【図１０】

本発明の実施例のテーブル構成（２）を説明する図

（A）

27

内線B	00　主回線 01 02　RSA管理 ・ ・

（B）

28

宛先コード
01181 71 70 ・ ・

（C）

28A

発番号
71493076600 32455673211 56427637150

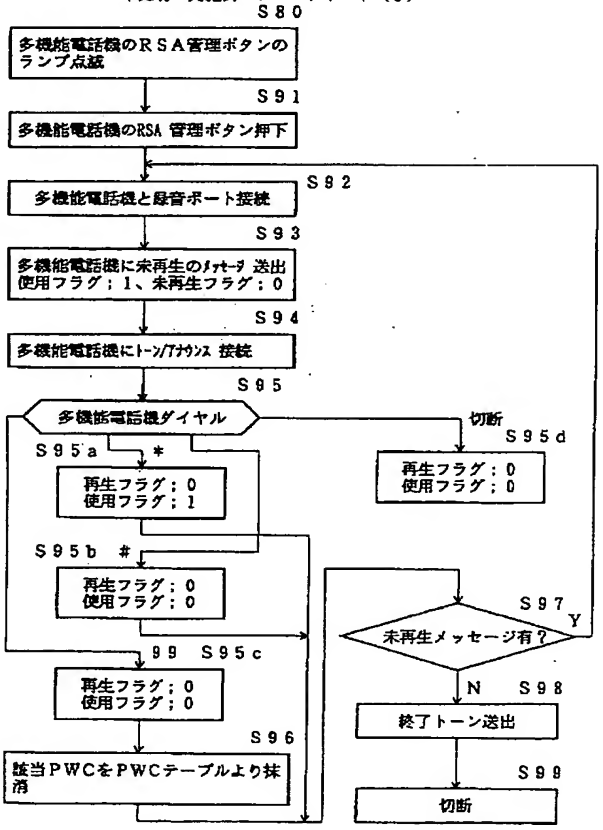
（D）

29

メッセージ番号	使用フラグ	PWC	ダイヤル番号	日時	再生フラグ
001 002	1 0	4589 7932	01181 711235		0 0

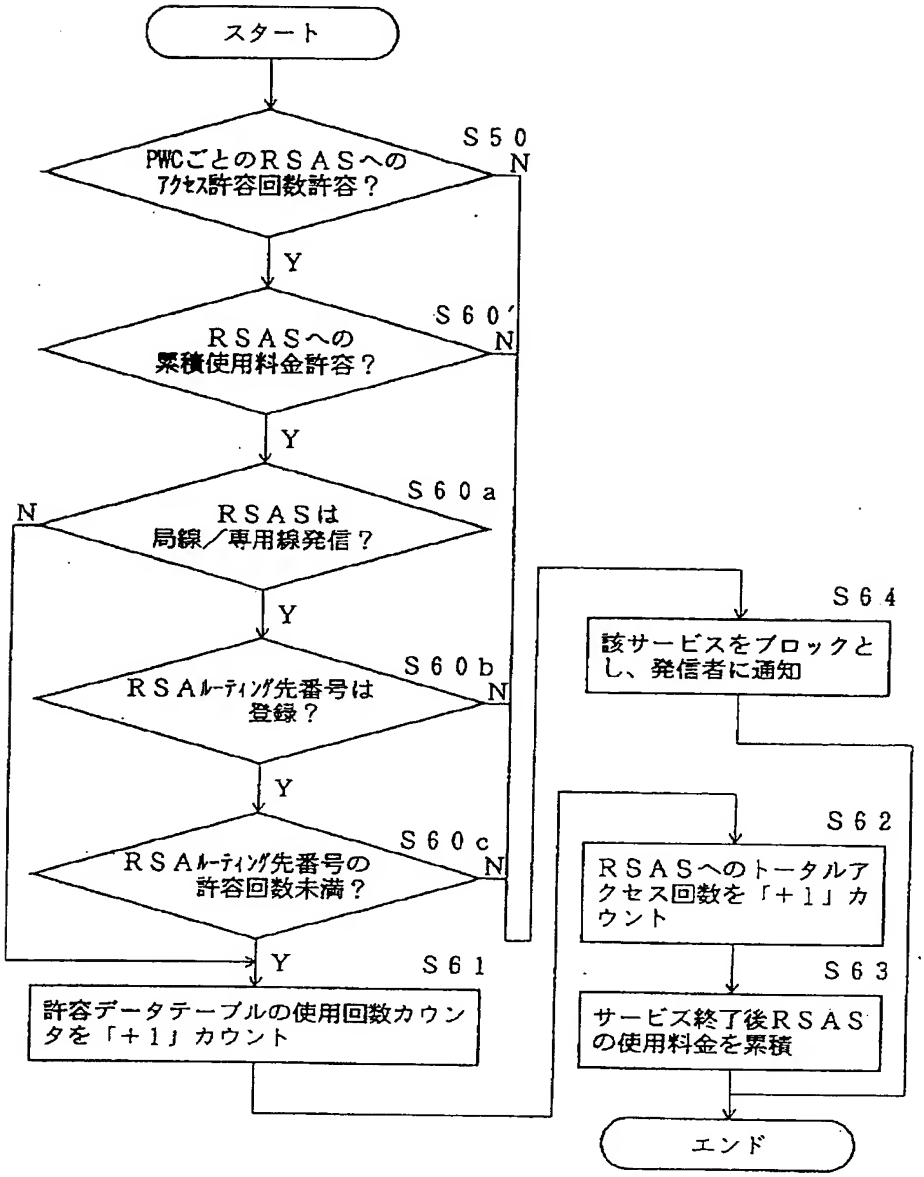
【図１２】

本発明の実施例のフローチャート（５）



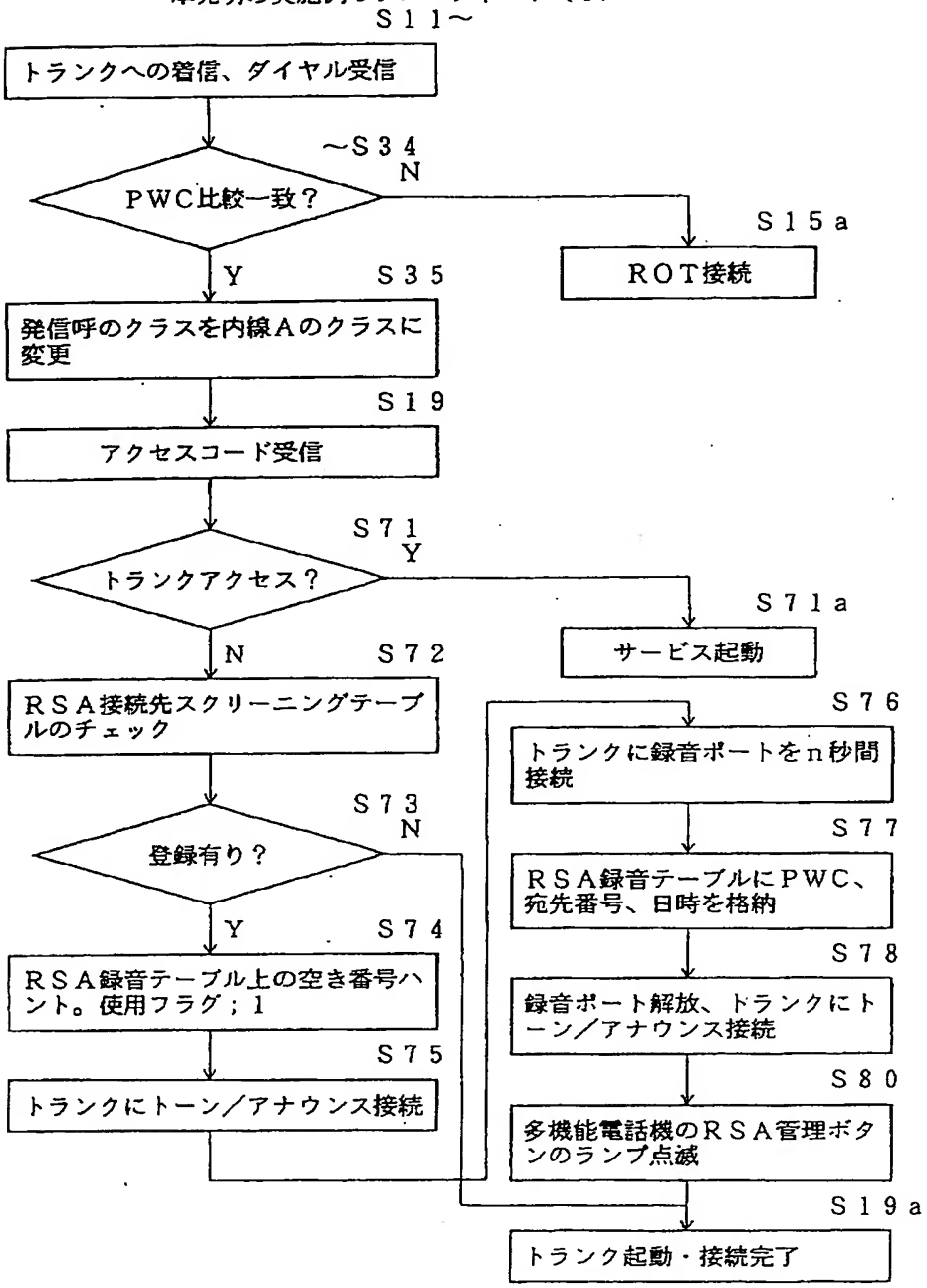
【図８】

本発明の実施例のフローチャート（３）

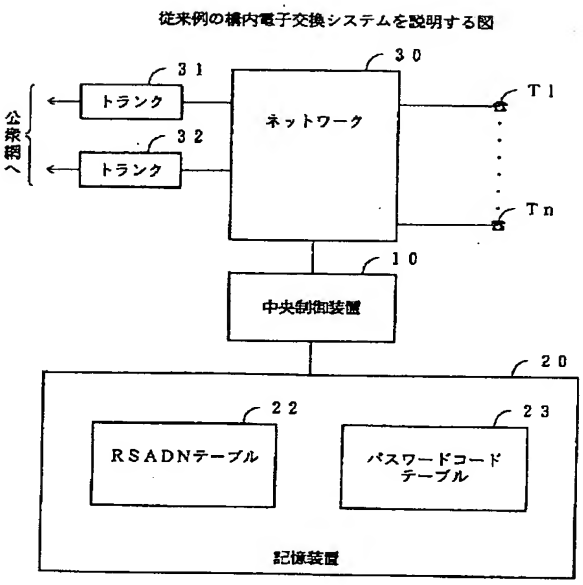


【図１１】

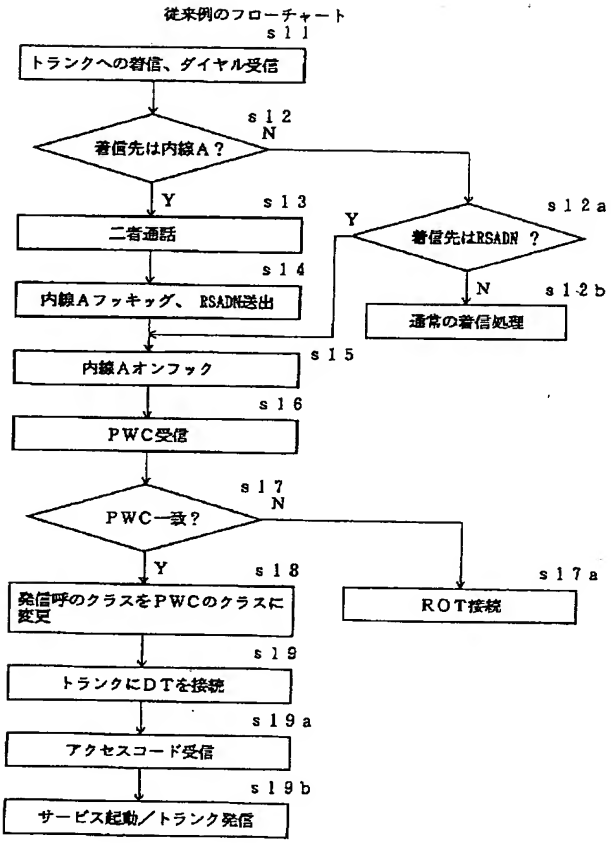
本発明の実施例のフローチャート（４）



【図１３】


従来例の構内電子交換システムを説明する図
公衆網へ
31
トランク
32
トランク
30
ネットワーク
T1
Tn
10
中央制御装置
20
22
RSADNテーブル
23
パスワードコード
テーブル
記憶装置

【図１４】


従来例のフローチャート
s11
トランクへの着信、ダイヤル受信
s12
着信先は内線A？
N
Y
s13
二者通話
s12a
Y
着信先はRSADN ？
N
s12b
通常の着信処理
s14
内線Aフッキング、 RSAD#送出
s15
内線Aオンフック
s16
PWC受信
s17
PWC一致？
N
Y
s18
発信呼のクラスをPWCのクラスに変更
s17a
ROT接続
s19
トランクにDTを接続
s19a
アクセスコード受信
s19b
サービス起動／トランク発信